2016 Internet2 Trust and Identity Accomplishments

February 28, 2017

Table of Contents

Executive Summary

The new Internet2 Trust and Identity Division completed its first full year in 2016, starting with the January appointment of Kevin Morooney as vice president and ending with a production candidate release of the Trust and Identity in Education and Research (TIER) software. This 2016 Trust and Identity report has five major themes, which are summarized here. This report also provides a review of the Internet2 Trust and Identity community accomplishments during the year.

1. **Positioning for the Future** - A major community effort helped set the direction for Internet2 Trust and Identity, including both InCommon and TIER (Trust and Identity in Education and Research). A series of meetings reviewed service offerings and capacity, the resulting gaps, and the need for financial sustainability. Internet2 also conducted a marketing and segmentation study of InCommon and a community review of the InCommon Certificate Service.

2. **Expanding the Boundaries of Federation** - Two major efforts during 2016 involve expanding the reach of the InCommon Federation, including integrating with the GÉANT's global eduGAIN interfederation service. Thanks to a strong partnership with MCNC, we kicked off a proof of concept of the Steward Program to extend federation to K-14 (K-12 and community colleges).

3. **Raising Trust and Interoperability** - Community members led activities in 2016 to raise the trust level and to increase interoperability across the InCommon Federation. The Assurance Advisory Committee proposed a set of Baseline Expectations for Trust in Federation (subsequently approved by InCommon Steering) and also developed a Multifactor Authentication Interoperability Profile. The InCommon Federation started a proof of concept of the global SIRTFI (Security Incident Response Trust Framework for Federated Identity) program and began efforts to move to an alternative to the large metadata aggregate distribution system (e.g. per-entity metadata).

4. **Trust and Identity for Education and Research (TIER) Releases** - The Internet2 TIER Program issued its first two software releases during 2016. TIER packages three open-source software components together (COmanage, Grouper, and Shibboleth) and includes a number of campus practices. The goal is to provide an open-source identity and access management suite developed by and for research and education.

5. **Engaging the Community** - Community working groups continue to help Internet2 Trust and Identity make progress on a number of fronts (as documented throughout this report), as well as serving as the major way to engage the community. Other successful programs continued during 2016, including the monthly IAM Online webinar series, Shibboleth Installation Workshops, and the Internet2 Global Summit and Internet2 Technology Exchange meetings.

Major Themes

- Positioning for the Future
- Expanding the Boundaries of Federation
- Raising Trust and Interoperability
- Trust and Identity for Education and Research (TIER) Releases
- Engaging the Community

Positioning for the Future

In early 2016, Internet2 Trust and Identity leadership developed a projection of staffing resources needed to support sustainable and scalable development and operations of the newly minted division. Subsequent meetings and conversations with were held with the community to do a reality check of the assumptions. Below are the conclusions of the three primary engagement sessions.

Charting the Path Forward - TIER and InCommon

Several small leadership groups drawn from the trust and identity community met to discuss expectations for InCommon, TIER, and Internet2 Trust and Identity overall. These groups reviewed current service offerings and capacity, the resulting gaps, and the need for financial stability.

The TIER and InCommon Path Forward teams aligned and expressed these common observations and findings:

- Internet2/InCommon/TIER have a leadership position in US trust and identity. There is a desire to maintain this position, even in the face of considerable threats.
- The trust and identity solution set(s) for higher education remain sufficiently unique that we need to continue to develop these solutions.
- The InCommon Federation and TIER Program are highly dependent upon one another.
- Sustained engagement with both executive and technical community leadership will be necessary for a vibrant trust and identity set of capabilities and vetted campus deployment strategies.
- Services and new capabilities require multiple funding strategies that best suit their contexts.
- Financial subsidization of a service or new capability should be an intentional temporary bridging strategy; otherwise they should stand on their own.

The TIER Path Forward team had these conclusions about TIER:

- Solidify the newly created role of Vice President of Trust and Identity within Internet2 and move to a permanent governance structure. This will include the move towards a Trust and Identity Program Advisory Group (PAG) and require broad communication and listening across all stakeholders.

- Continue development and achieve sustainability for components that increase velocity and efficiency of the program and expand its reach: de/provisioning, entity registry (person and object), components packaging, components and operations security audit.
- Continue development and achieve sustainability for Shibboleth, Grouper, and application programming interfaces (APIs) for ease of campus integration.
- Continue management of the program and leverage Internet2's existing strengths (community engagement, communications and marketing, program management, etc.) in other areas to augment these efforts.

The InCommon Path Forward team identified these priorities:

- Sustaining the Shibboleth Federating and Single Sign-on software is required for ensuring the evolution of the core federation services (e.g. support for OpenID Connect).
- Hardening and sustaining federation operations is important. We need to achieve an acceptable risk profile reflective of participant dependency on the federation, including disaster recovery and business continuity, software quality assurance processes, and scheduled security reviews.
- Scaling the federation operations and infrastructure for the future to address critical items such as metadata exchange and delivery and adoption of campus requested services such as OpenID Connect.
- Maturing the federation service delivery to ensure a positive participant experience and to enable scaling up to support a broader set of participants, such as a ticketing system and the Steward Program (which allows for increased participation by K-12 through collaboration with regional and state networks).
- Creating and adhering to standards of interoperability, security, and trust practices aligned with the interests of all participant communities to increase the ease of connecting to and value of the federation.

The InCommon Steering Committee further discussed this last set of recommendations and concluded that additional funding was needed very quickly to address security and operational gaps. The InCommon fees were increased in November 2016, to take effect for the 2017 operating year.

InCommon Marketing and Segmentation Study

In parallel to its mission to serve the broad education sector, the demographics of InCommon participants have changed over the last several years, with significant increases in the number of companies (many of them small) and smaller colleges and universities. In order to understand the expectations and needs of its participants, particularly in light of these changes, Internet2 commissioned a marketing and segmentation study of InCommon, which will be completed during the first quarter of 2017.

InCommon Certificate Service Review

The InCommon Certificate Service was established in 2010 as a way to significantly reduce costs and increase flexibility in the use of a variety of digital certificates (SSL, client, extended validation and others). The program now has 389 subscribers (see Appendix A for a year-by-year look at subscribers). During July 2016, a working group completed a review and identified desired features and improvements for the next generation of the service.

Expanding the Boundaries

The InCommon Federation reached across the globe this year and began a Proof of Concept to investigate scaling to include K-14 in the Federation.

Global Interfederation: eduGAIN

Since the formation of the InCommon Federation in 2005, a top goal has been to enable international collaboration for U.S. research and education. In February 2016, the Federation went into production with eduGAIN, the global interfederation service operated by GÉANT that enables seamless access to global services to all its participants. As of the end of 2016,39 international federations participate in eduGAIN, offering convenient single sign-on interaction with higher education institutions, research organizations, and corporate Service Providers around the world.

Global interfederation touched almost every aspect of InCommon Federation operations and affected all 834 (at the time) participating organizations. eduGAIN took four years to plan, with an intensive documentation, legal, technical, communication, and education effort during the last nine months of that time span. The InCommon Federation trust infrastructure (metadata aggregate) increased significantly in size, from 17MB on February 14, 2016, to 33MB the following day when the Federation began importing eduGAIN metadata.

InCommon Steward Program Proof of Concept

InCommon and MCNC (North Carolina's regional network services provider) completed a community review of the InCommon Steward Program and embarked on a proof of concept. The program is a scalable way to extend federated identity to K-14. In late December 2016, Internet2 and MCNC staff met in North Carolina to discuss each organization's role in the Steward process and ensure that MCNC's onboarding and trust registry procedures match those of the InCommon Federation. The proof of concept will continue through June 2017.

Raising Trust and Interoperability; Driven by Research

Raising trust was a key goal this year and was driven by the increasing needs for security, alignment, and interoperability to support research.

Increasing Trust: Baseline Expectations Approved

The InCommon Steering Committee approved a set of Baseline Expectations for Trust in Federation developed by the InCommon Assurance Advisory Committee and reviewed by the community. The policy includes expectations for Identity and Service Provider Operators, as well as the Federation Operator. The expectations establish a "floor" for trust across the InCommon community and are expected to form the basis for replacing the InCommon POP (Participant Operating Practices), which requires participants to publish their practices. The next step involves developing an implementation plan.

Federated Security Response Proof of Concept

International research organizations along with REFEDS (the research and education federation operators), drafted a specification for a federated incident response framework called SIRTFI (Security Incident Response Trust Framework for Federated Identity). It includes a list of assertions that would be self-attested by an organization. One key requirement is publishing organizational security contacts in metadata and Internet2 Trust and Identity initiated a process for moving all security contacts in metadata to the REFEDS specification. Also, the InCommon Federation is conducting a SIRTFI proof of concept with several Identity and Service Provider Operators.

Research & Scholarship Category Progress

InCommon continues to promote the Research & Scholarship (R&S) Category of Service Providers as a way to make attribute release, and easier across the Federation for collaboration services. When a user accesses R&S services, their Identity Provider releases a small set of attributes to those services. Some InCommon Identity Providers (to date, 85) release this set of attributes only to R&S SPs registered by InCommon, while others (to date, 46) release to any R&S SP, including those registered by other federations. The latter makes it easier for researchers to access international collaboration services and InCommon is actively encouraging IdPs to migrate to the global version.

Alternatives to the Metadata Aggregate

During 2016, the Per-Entity Metadata Working Group evaluated the use of per-entity metadata distribution as an alternative to the current metadata aggregate and developed a list of requirements for such a service. This new service enables Identity Providers and Service Providers to download only the metadata they need to federate with their partners instead of the entire aggregate. The working group recommends deploying a per-entity service with an availability of 99.99%, providing education and communication about adoption, and work with SAML software developers to ensure compatibility. The group also recommended InCommon place an interim IdP-only metadata aggregate into production to address short term needs of research Service Providers, which was completed in October.

Federation Interoperability Profile Moves to Kantara

The InCommon Federation Interoperability Working Group developed the SAML V2.0 Implementation Profile for Federation Interoperability, containing minimal and best practice statements to improve interoperability by default. The profile was then transitioned to the Kantara Initiative for long-term stewardship. The Kantara Federation Interoperability Working Group has taken up this work as the next step toward publishing and promulgating the profile as a Kantara recommendation across sectors in addition to research and education.

Multifactor Authentication Profile

The InCommon Assurance Advisory Committee proposed and developed a Multifactor Interoperability Profile for Service and Identity Providers to use to communicate the need for and use of MFA at the time of the transaction. This Profile is under review by REFEDS to ensure international use and interoperability.

Shibboleth IdPv3 Upgrade Progress

InCommon Operations made a concerted effort during 2016 to encourage Identity Providers to upgrade to version 3 of Shibboleth Identity Provider (IdPv2 went end-of-life in July 2016). For a list of up-to-date IdPs, see Shibboleth Identity Providers.

InCommon Certificate Service Adds ECC Certificates

The InCommon Certificate Service announced the availability of ECC (Elliptical Curve Cryptography) certificates. ECC certificates provide an alternative to RSA keys, which keep increasing in size to maintain cryptographic strength.

TIER Software Releases and Key Accomplishments

The TIER Program (Trust and Identity in Education and Research) issued its first two software releases during 2016. TIER packages three open-source software components together (COmanage, Grouper, and Shibboleth) and includes a number of campus practices. The goal is to provide an open-source identity and access management suite developed by and for research and education.

The first TIER release, delivered in April 2016, provided a look at the packaging strategy of using virtual machine images and Docker containers for software distribution. The second release in December 2016 is a production candidate that includes virtual machine images preloaded with the Docker containers. TIER has moved to a continuous release pipeline, with updates and changes provided when they are available, as opposed to waiting for specific release dates, enabling adopters to leverage new capabilities continuously.

The TIER software requirements and development result from significant work by the community. For example, during 2016, the community participated in 259 working group calls for a total of 2,927 hours (assuming 8-hour days, that's 366 person-days!).

See the TIER Community Resources web page for details, including the process used for developing requirements, community working groups, interoperability profiles, and other resources.

Community Development of The DevOps Process

The TIER community has defined and adopted a DevOps process for continued development of the software and practices. DevOps is the practice of operations and development engineers participating together in the entire service lifecycle, from design through development to production. The themes for TIER development are: 1) to build components, processes and practices in the most reliable, management, and predictable manner possible; and 2) produce secure, dependable, extensible, and flexible solutions that can be easily maintained by campus practitioners. This blog post provides the background and details.

TIER Reference Architecture Defined

A team of TIER architects defined a "reference architecture" for the higher education community to use as a guide for TIER development. A Reference Architecture is a set of diagrams and supporting text that describe the functional components in an overall distributed system. The TIER Reference Architecture shows components specifically for identity and access management in a higher education institution, and shows their relationship to one-another. This blog post provides details and a diagram.

TIER Demonstrations at TechEx 2016

Live presentations at TechEx 2016 highlighted the work and key developments being produced by TIER working groups and component architects. These well-received demonstrations provided community members deeper insight into the current TIER development efforts and how the TIER architecture and software components can help their institutions adapt the growing IAM challenges. This blog post provides details about the demonstrations.

TIER Grouper Deployment Guide

A group of TIER developers and architects is developing a Grouper Deployment Guide, intended to provide technical guidance for an initial deployment of Internet2 TIER Grouper component. This guide is expected to provide a model for similar documents for other TIER components.

Engaging the Community

Trust and Identity convenes the community to develop requirements, specifications and program activities in the form of 17 working and advisory groups over the year. In addition to these important engagements, the community participated in several educational opportunities.

Videos Summarize Trust and Identity, InCommon, and TIER

Internet2 produced a video that provides a high-level overview of trust and identity and was designed to help participants quickly introduce such concepts as federated identity to colleagues, other stakeholders, and potential partners. Another video includes trust and identity experts discussing the goals of the TIER program.

Education Programs

IAM Online Webinar Series

The monthly IAM Online webinar series marked its seventh year of operation in 2016. Appendix D includes a list of topics, speakers, and number of attendees during 2016. Altogether 596 viewers attended these 7 sessions of IAM Online.

InCommon Shibboleth Installation Workshops

The InCommon Shibboleth Installation Workshops marked the seventh year of operation. Four workshops took place in 2016 with a total attendance of 134. See Appendix E for details.

2016 Internet2 Global Summit

The 2016 Internet2 Global Summit included “identity morning,” with a joint meeting of the two leading trust and identity advisory groups (InCommon Steering and the TIER Community Investor Council). The groups reviewed a number of trust and identity programs, including eduGAIN, the status of the Shibboleth Consortium, and the first TIER release. The Global Summit also brought together TIER working groups and architects to review the TIER release and discuss plans for the next version.

2016 Internet2 Technology Exchange

In its third year, the Internet2 Technology Exchange has become established as an important technical meeting for trust and identity in research and education in the U.S., with a significant global component and attendance. The trust and identity community combined three focused meetings into the 2016 TechEx: REFEDS, the conference for research and education identity federations worldwide; Advance CAMP, the unconference meeting that explores just-in-time issues and challenges of community-wide interest or concern; and two tracks of CAMP, with campus-focused sessions comprised of community proposals. More than 170 trust and identity professionals attended.

Open ID Connect Workshops for SAML Architects

Internet2 hosted two hands-on workshops on OpenID Connect during February 2016, aimed at SAML architects and others wanting significant technical exposure to OpenID Connect, which is an emerging standard and will play a role in Internet-scale authentication and authorization.

Engaging the Community: Working Groups

Appendix C includes a list of the working groups, chairs, links to wiki pages, and a summary of their charters and any reports or other results.

TIER Community Investor Council (TCIC)

In 2015, 49 colleges and universities made a three-year financial commitment for TIER and formed the TIER Community Investor Council (TCIC) to guide planning and development. Internet2 provides the day-to-day management and staffing of TIER software development, support for community working groups, and development of community practices. The TCIC sets the stage for the long-term sustainability of TIER, addressing both funding and governance.

TIER Ad Hoc Advisory Group

The TIER Ad Hoc Advisory Group is a short-term Internet2 technical strategy group to help instantiate the community requirements, specification and adoption process portion of TIER. The Group is shepherding the creation of a standing architecture strategy group for Internet2 Trust and Identity called CACTI (Community Architecture for Trust and Identity).

InCommon Steering Committee

The InCommon Steering Committee is the policy body for the InCommon Federation and related services. During the past year, the Steering Committee has focused on the development of InCommon priorities, strengthened the relationship between InCommon and the TIER Program, enacted a new privacy policy, and worked on policy matters related to eduGAIN, the Steward Program, and Baseline Expectations.

InCommon Assurance Advisory Committee

The InCommon Assurance Advisory Committee (AAC) is the oversight body for the InCommon Identity Assurance Program, which provides policies and frameworks for increasing trust across the federation. The AAC has identified the InCommon POP (Participant Operating Practices) as a barrier to the adoption of assurance profiles and is exploring alternatives. The AAC also developed a set of “baseline expectations” for IdPs, SPs, and Federation Operators, and developed a Multi-factor Interoperability Profile for Service and Identity Providers to use to communicate the need for and use of MFA at the time of the transaction.

InCommon Technical Advisory Committee

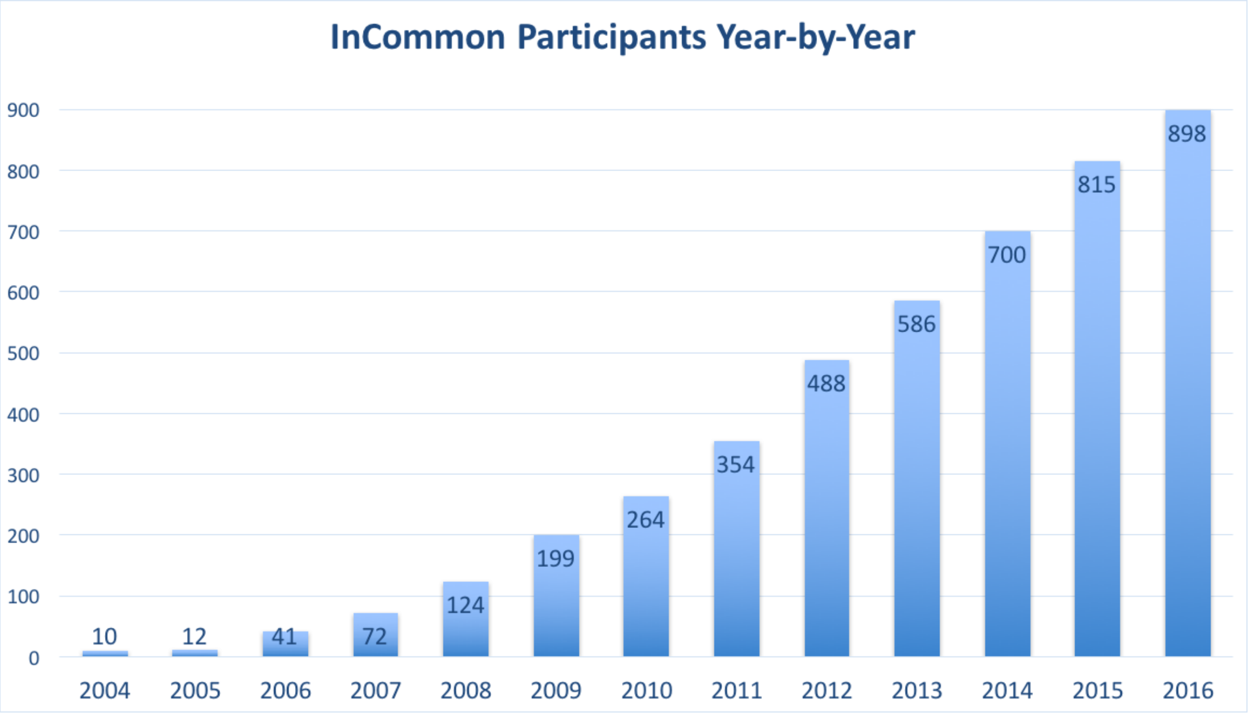
The InCommon Technical Advisory Committee (TAC) had a busy year, with work related to eduGAIN, chartering working groups to explore federation interoperability, multifactor authentication, the use and potential use of external identities on campus and in the Federation, and improving access through the use of service categories like Research & Scholarship.

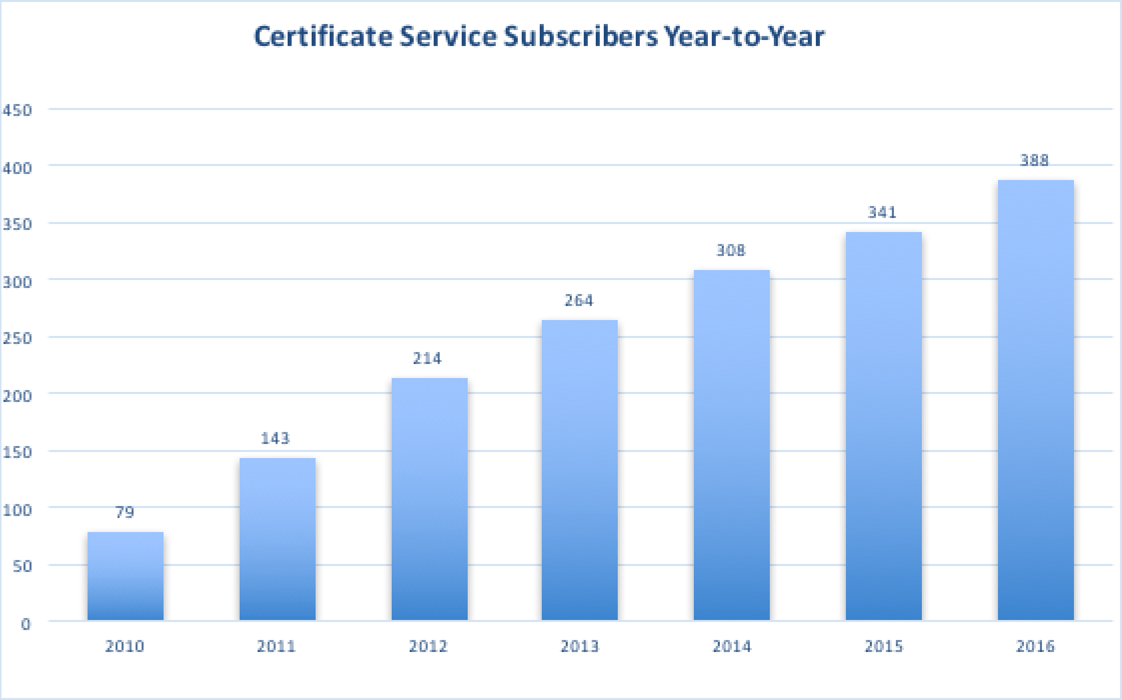
InCommon and TIER Working Groups

InCommon Working Group	Chair	Working Group Materials
OIDC Survey Working Group	Albert Wu, UCLA	https://spaces.internet2.edu/x/pIIQBg
Deployment Profile Working Group	Keith Wessel, University of Illinois Urbana-Champaign	https://spaces.internet2.edu/x/WoIQBg
Per-Entity Metadata Working Group	Scott Koranda, LIGO	https://spaces.internet2.edu/x/T4PmBQ
Federation Interoperability Working Group	Walter Hoehn, University of Memphis	https://spaces.internet2.edu/x/ioRRBQ
Certificate Service Review Working Group	Chris Bongaarts, University of Minnesota	https://spaces.internet2.edu/x/s4RRBQ
Multifactor Authentication (MFA) Interoperability Profile Working Group	Karen Herrington, Virginia Tech	https://spaces.internet2.edu/x/CY5HBQ

TIER Working Group	Chair	Working Group Materials
TIER Data Structures and APIs Working Group	Keith Hazelton, University of Wisconsin-Madison	https://spaces.internet2.edu/x/SgFwBQ
TIER Packaging Working Group	Jim Jokl, University of Virginia	https://spaces.internet2.edu/x/JYV4BQ
TIER Security and Audit Working Group	Helen Patton, The Ohio State University	https://spaces.internet2.edu/x/3gHSBQ
TIER Entity Registry Working Group	Warren Curry, University of Florida Benn Oshrin, Spherical Cow Group	https://spaces.internet2.edu/x/gYKeBQ
TIER Component Architects Working Group	Steve Zoppi, Internet2	https://spaces.internet2.edu/x/RAFwBQ

Appendix A: Statistics





Appendix B: Newsletters and Blogs

InCommon Update Newsletters

InCommon published 12 monthly newsletters during 2016, highlighting news of interest to InCommon execs and InCommon site administrators, and InCommon Certificate Service subscribers.

December 2016
November 2016
October 2016
September 2016
August 2016
July 2016
June 2016
May 2016
April 2016
March 2016
February 2016
January 2016

TIER Newsletters

The TIER program publishes a periodic newsletter with updates and details about the work accomplished by the TIER working groups. TIER published 10 newsletters during 2016

December 2016
November 2016
September 2016
August 2016
July 2016
June 2016
May 2016
March 2016
February 2016
January 2016

TCIC Chair Blog

Each TIER newsletter includes a blog from the TCIC chair, providing an update on the key activities and accomplishments in the TIER program.

December 2016 - 2016 Year in Review
November 2016 - Paths Forward are now Paths in Progress
September 2016 - TIER Governance Meetings at the 2016 Internet2 Technology Exchange
August 2016 - Paths Forward for Trust and Identity: Conclusions of Summer Planning
July 2016 - Paths Forward to the Future

June 2016 - Common Principles, Sustainability Key to TIER Success
May 2016 - TIER Release One
March 2016 - Release One: We Need You
February 2016 - Gravitational Wave Research, Federation and TIER
January 2016 - Managing Identities in the Digital Age

Trust and Identity Blogs

Exploring the World of Metadata
InCommon and TIER: Better Together, Part 1
InCommon and TIER: Better Together, Part 2
The Landscape of DevOps
TIER Reference Architecture
TIER Supports the Weave of Research and Education

TIER Community Contributor Spotlights

The monthly TIER newsletter includes a community contributor spotlight in each issue. These are the people featured in one of the newsletters during 2016.

Rob Carter, Duke University□
Gabor Eszes, Old Dominion University
Michael Hodges, University of Hawaii
Bill Thompson, Lafayette College
Brian Savage, Boston College
Tom Jordan, James Babb and Jon Miner, University of Wisconsin-Madison □
Richard Biever, Duke University
Janemarie Duh, Lafayette College
Jim Fox, University of Washington
Warren Curry, University of Florida

Appendix C: Working Group Summaries

InCommon Federation Interoperability Working Group

Chartered by: InCommon Technical Advisory Committee
Chair: Walter Hoehn, University of Memphis
Wiki: https://spaces.internet2.edu/x/ioRRBQ

This working group developed a list of requirements for scalable interoperation for those developing SAML software to ensure that it interoperates with research and education federations such as InCommon and listed such requirements that could be tested in some type of framework. The working group delivered a final report in March 2016, including a profile that sets out software conformance requirements to improve interoperability within an identity federation (the SAML V2.0 Implementation Profile for Federation Interoperability). Kantara, a multi-sector identity-related standards and community group, has agreed to be the caretaker of the profile and for promulgation across key government and corporate sectors.

InCommon Certificate Service Review Working Group

Chartered by: InCommon Executive Director
Chair: Chris Bongaarts, University of Minnesota
Wiki: https://spaces.internet2.edu/x/s4RRBQ

This working group reviewed and provided input on matters pertaining to the next generation InCommon Certificate Service. Members reviewed a number of short-term tactical issues, conducted a community survey, and provided a list of desired features for the next generation certificate service. The working group has conducted the survey and is writing its final report.

InCommon Multifactor Authentication (MFA) Interoperability Profile Working Group

Chartered by: InCommon Assurance Advisory Committee
Chair: Karen Herrington, Virginia Tech
Wiki: https://spaces.internet2.edu/x/CY5HBQ

This working group developed a specification that enables Service Providers to request and for Identity Providers to be able to communicate that a person used another factor when authenticating. The group assembled use cases, developed a list of widely deployed MFA technologies, and defined requirements for the profile. For the TIER release in April 2016, the working group issued a number of documents for public review, including its final report, and an InCommon MFA Profile and an InCommon Base Level Profile.

InCommon OIDC Survey Working Group

Chartered by: InCommon Technical Advisory Committee
Chair: Albert Wu, UCLA
Wiki: https://spaces.internet2.edu/x/pIIQBg

This working group has surveyed the research and education community about the problems they are trying to solve with OIDC/OAuth2. The working group is collecting use cases and will summarize the findings and conclusions of the survey, as well as develop next steps for TIER, federating software, InCommon, and Federation-level support. The survey has been completed and the analysis is underway.

InCommon Deployment Profile Working Group

Chartered by: InCommon Technical Advisory Committee
Chair: Keith Wessel, University of Illinois, Urbana-Champaign
Wiki: https://spaces.internet2.edu/x/WoIQBg
This working group was chartered to develop a deployment profile that describes required and recommended practices for IdPs and SPs operating in the research and education community. To date, the working group has categorized and refined the list of issues to be considered in a deployment profile.

InCommon Per-Entity Metadata Working Group

Chartered by: InCommon Technical Advisory Committee
Chair: Scott Koranda, LIGO
Wiki: https://spaces.internet2.edu/x/T4PmBQ
The Per-Entity Metadata Working Group was chartered to evaluate the use of Per-Entity Metadata as an alternative to the current metadata aggregate, to address issues of performance, and develop requirements for a production per-entity metadata service. The working group recommends deploying a per-entity service with an availability of 99.99%, providing education and communication about adoption, and work with SAML software developers to ensure compatibility.

TIER Data Structures and APIs Working Group

Chair: Keith Hazelton, University of Wisconsin-Madison
Wiki: https://spaces.internet2.edu/x/SgFwBQ
This working group focuses on developing and implementing APIs for the main TIER components. Early in the year, the group decided to use Swagger 2.0 for its API specifications and to assign a representative to the Open API Initiative (which curates Swagger) to speak to the needs of research and education.

The group first worked on a Grouper API and spun up a smaller cohort to develop a Grouper Deployment Guide, which will take a new Grouper deployer through initial deployment and configuration. The TIER version of such a guide will provide community vetted recommendations and strategies for a TIER-compatible deployment.

The working group also provided a demo at the Internet2 Technology Exchange in September 2016, and is working on developing instrumentation to allow campuses to monitor how their components are behaving and how users are interacting with the software.

TIER Packaging Working Group

Chair: Jim Jokl, University of Virginia
Wiki: https://spaces.internet2.edu/x/JYV4BQ
The Packaging Working Group started the year by conducting an extensive survey focused on the necessary campus infrastructure to support and manage deployments and default configurations for TIER’s initial Shibboleth, Grouper, and COmanage components. The survey

showed a general trend away from dedicated and virtual machines and towards containers, appliances, and cloud services. As a result, the working group identified the use of Docker containers as a key direction for packaging the TIER components. The group also defined and put into place (TIER Production Release Candidate - December 2016) a continuous integration pipeline to allow for software updates as they are available, as opposed to waiting for a set release date. The working group also started discussion concerning Shibboleth IdP configuration management and is evaluating CANARIE's IdP installer as a potential solution.

TIER Security and Audit Working Group

Chair: Helen Patton, The Ohio State University
Wiki: https://spaces.internet2.edu/x/3gHSBQ
This working group developed recommendations for secure TIER development processes, best practices for ongoing security testing, and operational security processes such as change management, incident response, logging for audit purposes, and data lifecycle management. The group also reviewed InCommon operations and incident security proposals; in particular the proposed InCommon Incident Handling Framework.

TIER Entity Registry Working Group

Chairs: Warren Curry, University of Florida; Benn Oshrin, Spherical Cow Group
Wiki: https://spaces.internet2.edu/x/gYKeBQ
This working group drafted Identity Management Product Feature Details, an extensive review of TIER requirements and how those needs map to the features of available open source and commercial IdM applications. This analysis will guide development efforts and identify candidates for inclusion in upcoming TIER functionality. The working group also developed a Reference Architecture, which demonstrates how TIER components will work together in various use cases. The working group developed a test bed, which is a representation of a federation campuses can use for testing.

TIER Component Architects Working Group

Chair: Steve Zoppi, Internet2
Wiki: https://spaces.internet2.edu/x/RAFwBQ
The TIER Component Architects Working Group focuses on alignment of TIER processes, including the common core of technology platforms and tools. The group discusses approaches to translation issues, instrumentation direction, incentives to adoption, the DevOps workbench construction criteria, and coordination for TIER releases.

Appendix D: IAM Online Topics

IAM Online is a monthly series delivering interactive education on Identity and Access Management (IAM), sponsored by InCommon, Internet2, and the EDUCAUSE Higher Education Information Security Council.

Motivations and Policy Challenges of Multifactor Deployment
Presenters: Matthew Dalton (University of Massachusetts-Amherst), Brendan Bellina (UCLA)
Attending: 118

Paving the Way for Research Collaboration
Presenters: Chris Whalen (National Institute of Allergy and Infectious Diseases, NIH), Kathleen Fitzpatrick (Modern Language Association), Scott Koranda (LIGO), Von Welch (Center for Applied Cybersecurity Research)
Attending: 60

Grouper Enterprise Access Management
Presenters: Bert Bee-Lindgren (Georgia Tech), John Bryson (Georgia Tech), Madan Dorairaj (New York University), Chris Hyzer (University of Pennsylvania), Julio Macavilca (New York University), Carl Waldbieser (Lafayette College)
Attending: 107

Free the Attributes! Attribute Release, Scalable Consent, and User Convenience
Presenters: Rob Carter (Duke University), Ken Klingenstein (Internet2), Keith Wessel (University of Illinois, Urbana-Champaign)
Attending: 67

K-12 and Federation: Report from the Pilots
Presenters: Shaun Abshere (WiscNet), Bernie A’cs (National Center for Supercomputing Applications), Mark Beadles (OARnet), Scott Isaacson (Nebraska Educational Service Unit Coordinating Council), George Laskaris (NJEdge), Mark Scheible (MCNC), Ann West (Internet2)
Attending: 60

Registries and Records: The Ties That Bind an IAM System
Presenters: Warren Curry (University of Florida), Chuck Moore (Penn State), Renee Shuey (Penn State)
Attending: 118

InCommon Technical Work Updates and Plans

Presenters: C.W. Belcher (University of Texas-Austin), Chris Bongaarts (University of Minnesota), Steve Carmody (Brown University), Walter Hoehn (University of Memphis), David Walker (Consultant)

Attending: 66

Appendix E: InCommon Shibboleth Installation Workshop Locations and Attendance

2016	**Host**	**Attendees** **(max = 40)**
February	MCNC (Research Triangle, NC)	34
May	University of Chicago	34
June	Rochester Institute of Technology	28
October	California State University Chancellor’s Office	38
Total		134